Amendments to the Claims

This listing of claims will replace all prior version, and listings, of claims in the application.

Listing of Claims:

1. – 27. (Canceled)

28. (Currently Amended) A portable security device removably coupled to a computer system for selectively authorizing the computer system to use multiple items of protected information, comprising:

a processing unit;

at least one storage medium coupled to the processing unit;

an interface capable of receiving multiple items of authorization information that are associated with respective ones of the multiple items of protected information, wherein the multiple items of authorization information are stored within the at least one ~~memory~~storage medium; and

an interface program for selectively authorizing the computer system to use one of the items of protected information based upon the corresponding item of authorization information being stored in the ~~memory~~ storage medium.

29. (Previously Presented) The method of claim 28 wherein the multiple items of authorization information comprise key selectors.

30. (Previously Presented) The method of claim 29 a key is generated within the

portable security device based upon the key selectors and selective authorization is given to the computer system to use the multiple items of protected information based upon the key.

31. (Previously Presented) The method of claim 28 wherein the multiple items of authorization information comprise one or more secret keys.

32. (Previously Presented) The method for selectively authorizing the use of multiple items of protected information on a computer system using a portable security device that is removably coupled to the computer system, the method comprising the steps of:

(a) providing the portable security device with the capability of receiving multiple items of authorization information that are associated with respective ones of the multiple items of protected information, wherein the multiple items of authorization information are stored within a single memory in the portable security device; and

(b) selectively authorizing the computer system to use one of the items of protected information based upon the corresponding item of authorization information being stored in the memory.

33. (Previously Presented) The method of claim 32 wherein the multiple items of authorization information comprise key selectors.

34. (Previously Presented) The method of claim 33 further including the step of:

generating a key within the portable security device based upon the key selectors and selectively authorizing the computer system to use the multiple items of protected information based upon the key.

35. (Previously Presented) The method of claim 32 wherein the multiple items of authorization information comprise one or more secret keys.

36. (Previously Presented) A method for selectively authorizing the use of multiple items of protected information on a computer system, the method comprising the steps of:

(a) providing a portable security device with at least one memory containing a shared secret and space for multiple key selectors, one key selector for each item of protected information, and at least one I/O port, whereby the key selectors can be downloaded into the security device, and communications can be established with the computer system;

(b) receiving by the portable security device an authorization request from the computer system to authorize use of a particular one of the items of protected information; and

(c) using the stored key selector corresponding to the particular one of the items and the shared secret to generate authorizing information, wherein the computer system validates the authorizing information and releases the particular one of the items of protected information for use.

37. (Previously Presented) The method of claim 36 further including the step of providing the key selectors to the portable security device memory using external information authorities within a secure transaction.

38. (Previously Presented) The method of claim 37 further including the step of receiving a random challenge from the information authority, using the shared secret to encrypt the response, and validating by the information authority the response by decrypting with the shared secret.

39. (Previously Presented) The method of claim 36 where the shared secret is an encryption key.

40. (Previously Presented) The method of claim 39 further including the step of transforming the received key selector into an authorizing key using the shared secret key.

41. (Previously Presented) The method of claim 40 where the authorization request is a randomly generated challenge number.

42. (Previously Presented) The method of claim 41 where the authorization information is generated by using the challenge and the authorizing key.

43. (Previously Presented) The method of claim 36 further including the step of encrypting the key selectors before storing in the portable security device memory.

44. (Previously Presented) The method of claim 43 further including the step of storing the key selectors in a merged pool in memory using a blending algorithm, whereby an individual key selector cannot be extracted from a specific location in memory.

45. (Previously Presented) The method of claim 36 further including the step of receiving the multiple items of information from multiple information authorities.